IB 04/52053

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.10.13

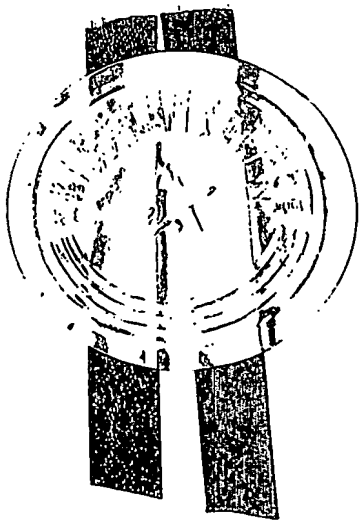
申　请　号：　2003101015909

申请类别：　发明

发明创造名称：　光盘、播放光盘的播放器及其播放方法

申　请　人：　皇家飞利浦电子股份有限公司

发明人或设计人：　彭杨、何达华、凯利·迪卡兰、牛顿·飞利浦、金盛



中华人民共和国
国家知识产权局局长　王景川

2004 年 9 月 28 日

权 利 要 求 书

1. 一种光盘，用来与下载的内容配合播放，该光盘具有一个公钥，该公钥是用来验证下载的内容是否是经过认证的内容。
2. 如权利要求 1 所述的光盘，其中该公钥是储存在该光盘的一个 BCAs 区内。
3. 如权利要求 1 所述的光盘，其中该公钥是储存在该光盘的一个媒体内容区内。
4. 一种光盘播放器，包括：

   一个读出装置，用来读出光盘的内容及公钥；

   一个网络接口，用来接收下载的相关内容；及

   一个验证装置，根据读出的光盘公钥来验证该下载的相关内容是否是经过认证的内容。
5. 如权利要求 4 所述的光盘播放器，还包括一个检测装置，用来检测下载内容的完整性，如果所检测的内容不是完整的，则不执行所述的验证。
6. 如权利要求 4 所述的光盘播放器，其中该下载的内容为应用程序。
7. 如权利 要求 6 所述的光盘播放器，其中该下载的应用程序为 JAVA 语言应用程序。
8. 一种播放方法，包括步骤：

   读出光盘的内容及公钥；

   下载相关的内容；及

   根据读出的公钥来验证下载的内容是否是经过认证的内容，以确认是否运行该下载的内容。
9. 如权利 要求 8 所述的播放方法，还包括对下载的内容进行完整性检测，以确认所下载的内容是否完整，如果不是完整的，则不执行所述的验证步骤；如果所检测的下载内容是完整的，则执行所述的验证步骤。
10. 如权利要求 8 或 9 所述的播放方法，如果经验证，下载的内容是没有经过认证的内容，则拒绝运行已下载的内容。
11. 如权利要求 10 所述的播放方法，如果经验证，该下载的内容是经过认证的内容，则运行下载的内容。
12. 如权利要求 8 所述的播放方法，其中该下载的内容为应用程序。
13. 如权利 要求 12 所述的播放方法，其中该下载的应用程序为 JAVA 语言应用程序。

14. 一种光盘，用来与下载的内容配合播放，该光盘具有一个部分，以用来验证下载的内容是否是经过认证内容。

15. 一种光盘，用来与网络服务器链接来实现播放，该光盘具有一个部分，用以与网络信息配合来验证光盘的播放权限。

16. 如权利要求 15 所述的光盘，其中该部分为储存在光盘中的公钥。

说 明 书

光盘、播放光盘的播放器及其播放方法

背景技术

本发明涉及一种光盘、播放光盘的播放器及其播放方法。

随着光盘及光盘播放技术的快速发展，越来越多的内容被储存到网络服务器上，以便在播放光盘的过程中将这些内容下载至播放器，以配合播放器播放光盘。

下载的内容可以是应用程序、音频、广告、游戏、动画及字幕等。其中应用程序是指JAVA语言所表达的应用程序或其它语言所表达的应用程序，而相较于其它语言，JAVA语言的平台无关性决定了其所表达的应用程序更为通用。JAVA 应用程序可以用来控制不同的播放器的播放，将其存至网络服务器上则为不同的播放器制造商提供更宽的商业平台，也给用户提供更灵活的应用。

将上述内容存至网络服务器上后，再随时下载至播放器来配合播放光盘，这种方式在很多光盘及相应播放器中均有应用，如蓝光光盘（Blu-ray Disc）及相应播放器、eDVD（enhanced DVD）及相应的播放器等。

目前，从网上下载内容的范围是由储存在光盘中的URLs（Uniform Resource Locator）列表（Walled Garden）来决定的，如果所下载的内容对应的 URLs 不在光盘储存的 URLs 列表中，则拒绝运行该下载的内容。

然而，存在光盘上的 URLs 列表所对应的内容只是经内容提供商确认是可以提供给用户使的，即直接存至网络服务器上，并没有经过认证。认证是指光盘内容提供商将与光盘相对应的内容存至网络服务器上时，由光盘内容提供商自己或者其它认证机构（CA，Certificate Authority，如微软公司的 Internet Explorer 及网景公司的 Navigator 等）确认可以提供给用户且加了私钥（Private key）的内容，私钥为大于或等于 500bits 的数字信息。

以上所述光盘内容提供商储存在网上的内容没有经过认证，则内容容易被其他人（如，黑客、盗版商及广告商等）所改动，而其 URLs 仍然与光盘储存的 URLs 列表上所列出的 URLs 对应，从而使得播放器运行了下载的内容，则极有可能对播放器及光盘内容造成破坏，以致给用户带来极大的麻烦。

还有可能是用户按照自己所需而输入的新 URLs 或播放过程中系统自动跳出的不名的 URLs（如，黑客、盗版商及广告商等提供的）。这些 URLs 如果和光盘所储存的 URLs 列表对应，而被播放器运行了，也有可能产以上所述同样的危害。

另外，如果内容提供商或内容提供商充许的第三方为用户提供了新的娱乐内容，即使该下载内容是用户所需的，且不会对光盘、播放器或光盘内容造成破坏，而该内容所对应的 URLs 不在光盘储存的 URLs 列表上，则仍然会被播放器拒绝运行该下载内容，此明显缩小了用户娱乐范围，也限制了内容提供者的商业模式。

因此，需要一种改进的光盘、播放光盘的播放器及其播放方法以避免上述缺陷。

发明内容

本发明提供了一种具有公钥（Public Key）的光盘。

本发明还提供了一种播放具有公钥的光盘播放器。

本发明也提供了一种播放具有公钥的光盘播放方法。

本发明所要解决的技术问题是通过以下技术方案来实现的：本发明所述的光盘，是用来与下载的内容配合播放。该光盘具有一个公钥

，该公钥是用来验证下载的内容是否是经过认证的内容。

本发明所述的光盘播放器包括一个读出装置、网络接口及一个验证模块。其中该读出装置是用来读出光盘内容及公钥；网络接口是用来接收下载的相关内容；而该验证模块是根据读出的公钥来验证该下载的内容是否是经过认证的内容。

本发明所述的播放光盘的播放方法，是在读出光盘内容及公钥且下载内容后，根据读出的公钥对下载的内容进行验证，以确认下载的内容是否是经过认证的内容。

由于采用了本发明所述的技术方案，本发明所述的光盘、播放光盘的播放器及其播放方法，是通过检测下载内容是否经过认证来确定是否运行下载的内容，因此，无论 URLs 如何变化，只要其所对应的内容是经过认证的均可以运行，即使所下载内容对应的 URLs 与光盘上所储存的 URLs 相对应，但是该下载的内容并未经过认证也将被拒绝运行，从而避免了运行带病毒信息而造成的影响，也提高了用户观看光盘的兴趣。

附图说明

图 1 是本发明一个实施例光盘及相关元件关系示意图；

图 2 是图 1 中光盘的结构示意图；

图 3 是图 1 中播放器的结构示意图；

图 4 是本发明一个实施例播放光盘的方法流程图。

下面参照附图结合实施例对本发明作进一步说明。

具体实施方式

图 1 所示，为本发明的一个实施例，该实施例中利用播放器 3 播放光盘 2，且播放器 3 与网络服务器 4 链接，以在播放过程中下载网络服务器 4 中的内容来配合光盘 2 上已存在的内容播放光盘 2。

下载的内容可以是应用程序、音频、广告、游戏、动画及字幕等。其中应用程序是指 JAVA 语言所表达的应用程序或其它语言所表达的应用程序，而相较于其它语言，JAVA 语言的平台无关性决定了其所表达的应用程序更为通用。JAVA 应用程序可以用来控制不同播放器的播放，将其存储至网络服务器上则为不同的播放器制造商提供更宽的商业平台，也给用户提供更灵活的应用。

且这些下载的内容均是经过认证的内容，即光盘内容提供商将与光盘相对应的内容存至网络服务器上时，由光盘内容提供商自己或者其它认证机构（CA，Certificate Authority，如微软公司的 Internet Explorer 及网景公司的 Navigator 等）确认可以提供给用户且加了私钥（Private key）的内容，私钥为大于或等于 500bits 的数字信息。因为有私钥的存在，这些下载的内容在网上不易被人修改。

图 2 所示为本发明一个实施例所披露的光盘 2 的结构示意图。该光盘 2 包括 BCAs（Burst Cutting Areas）区 22、导入区（Lead in）24 及媒体内容区（Media Content Areas）26。其中，BCAs 区 22 中包括一个公钥 23，公钥 23 是用来验证播放光盘 2 时下载的内容是否经过认证，与下载内容的私钥相对应且大于或等 500bit 的数字信息。

其中验证是通过非对称算法（如 Hash 算法等）来进行的，在这种算法中通过下载内容的私钥与光盘 2 的公钥 23 运算所得出一数字信息来实现的（详后述）。

图 2 所示的公钥 23 是位于光盘 2 的 BCAs 区 22，此仅仅为一个例子，该公钥 23 还可以位于光盘 2 的其它区域，如光盘的导入区 24 及光盘内容区 26 等。另外，图 2 仅出一个公钥 23，事实上，还可以有多个公钥 23，以分别指向整个光盘 2 的不同内容。光盘 2 的公钥 23 还可用来发送到网络服务器 4 中来获取播放光盘 2 的权限。

图 3 所示为本发明一个实施例所披露的光盘播放器 3。光盘播放器 3 包括网络接口 31、控制系统 32、驱动器 39 及输出装置 40。

其中控制系统 32 是用来控制光盘驱动器 39 及输出装置 40 的工作过程，且包括 RAM 33、ROM 35 及 CPU 38。RAM 33 中包括缓冲区 34，用来缓冲接收经网络接口 31 传递过来的下载内容。ROM 35 中包括检测模块 36 及验证模块 37，ROM 35 与 RAM 33 链接并接收 RAM 33 传递过来的下载内容。

CPU 38 是与 RAM 33 及 ROM 35 链接并控制 RAM 33 及 ROM 35 的工作过程。光盘驱动器 39 是在控制系统 32 的控制下用来读取光盘 2 的媒体内容及公钥 23，并将读出的公钥 23 传递至控制系统 32 中的 ROM 36，而将媒体内容传递至输出装置 40。

控制系统 32 中的检测模块 36 是用来检测缓冲区 34 传递过来的下载内容是否完整，如果不完整，则放弃运行下载的内容；验证模块 37 是在检测模块 36 检测出的下载内容是完整的情况下，用来验证下载的内容是否是经过认证的内容，其验证是利用是利用现今成熟的公钥体系算法及协议来实现的，比如通过下载内容中私钥的数字与光盘驱动器 39 传来的公钥 23 的数字运算关系，算得验证结果。举一个简单的例子，光盘 2 公钥 23 与下载内容私钥的关系为 $Y=B^x$，其中公钥 23 包括数字 Y 和 B，而下载内容的私钥为所包括的数字为 X，验证模块对 B^x 进行计算，如果计算结果就是 Y，即下载的内容通过了验证，并认为下载的内容是经过认证且可以执行播放的；如果计算结果不是 Y，即下载的内容未通过验证，播放器 3 则会拒绝执行下载的内容。输出装置是用来输出经光盘驱动器读出的 信息及经控制系统中输出的信息。上述各元件的作用均是在 CPU 34 配合下来实现的。

图 4 所示为本发明一个实施例所述的光盘播放方法的流程图。播放器 3 读出光盘内容及光公钥（S100）后，从网络服务器中下载与光盘内容相关的内容（S110）。

接着，对已下载内容进行完整性检测（S120），以确认下载的内容是否完整，如果不完整，则放弃运行下载的内容（S130）。

如果下载的内容是完整的，再利用所读出的光盘公钥 23 来检测下载的内容是否是经过认证的内容（S140）。如果是未经过认证的内容，则放弃运行下载的内容（S130）；如果是经过认证的内容，则直接运行已下载的内容（S150），从而实现与光盘 2 上的已储存的信息配合来播放光盘 2。

由于采用了本发明所述的技术方案，本发明所述的光盘、播放光盘的播放器及其播放方法，是通过检测下载内容是否经过认证来确定是否运行下载的内容，因此，无论 URLs 如何变

化，只要其所对应的内容是经过认证的均可以运行，即使所下载内容对应的 URLs 与光盘上所储存的 URLs 相对应，但是该下载的内容并未经过认证也将被拒绝运行，从而避免了运行带病毒信息而造成的影响，也提高了用户观看光盘的兴趣。

虽然已经结合特定实施例对本发明加以描述，然而根据前面的描述，许多替代、修改与变更对于本领域的技术人员来说是显而易见的。因此，本发明将包括所有落在后附的权利要求的构思与范围之内的这种替代、修改与变更。

说 明 书 附 图

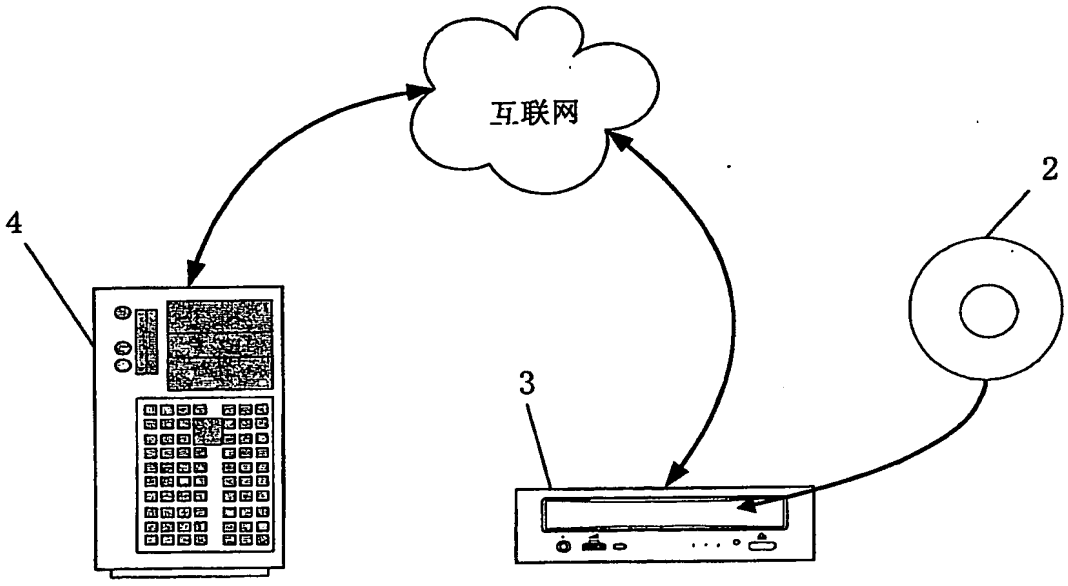


图1

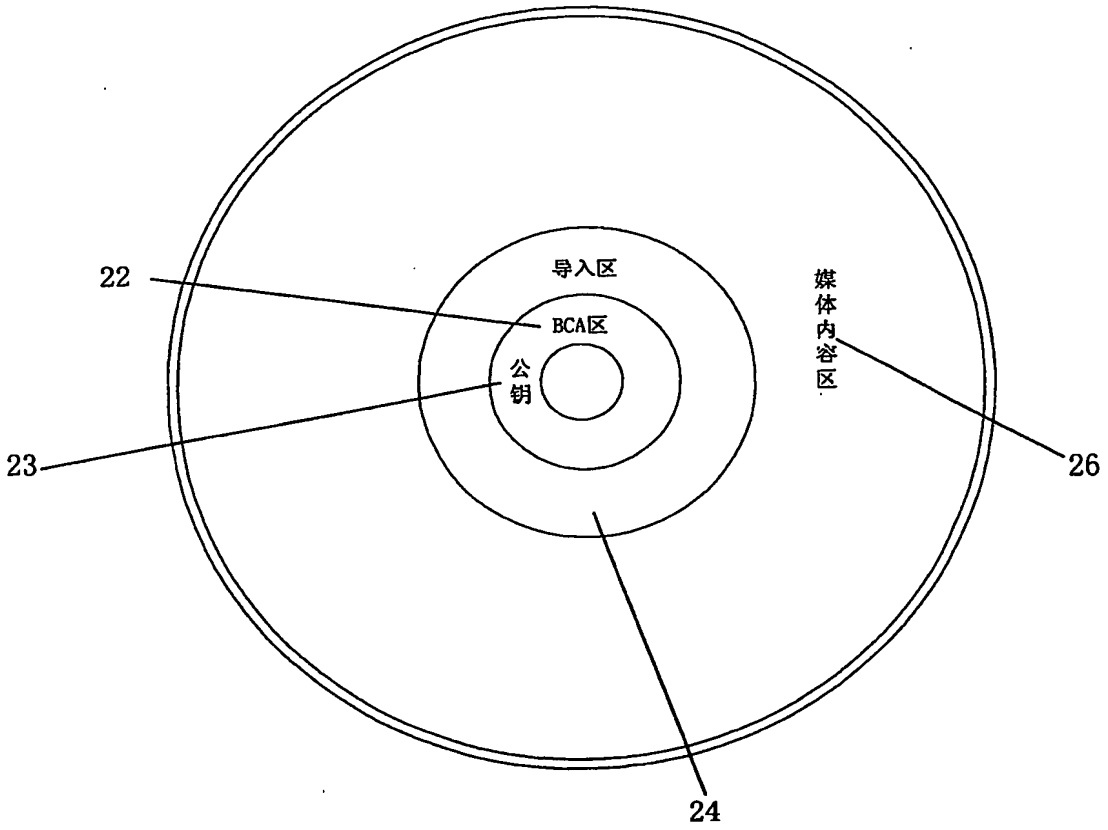


图2

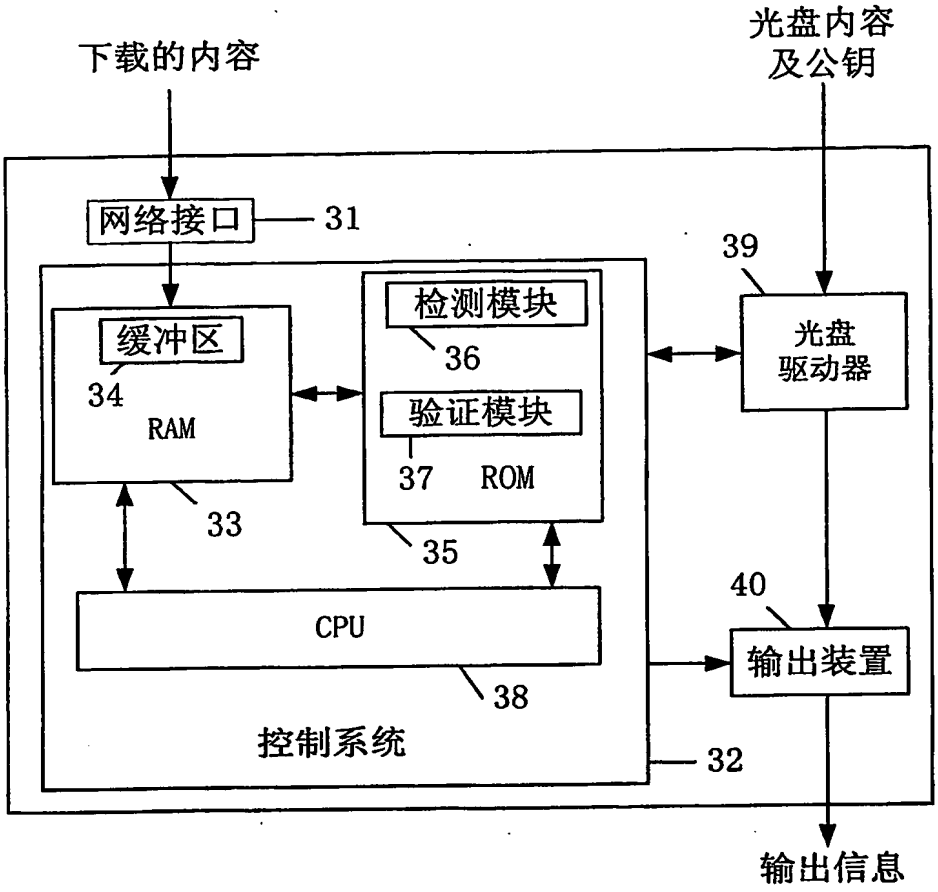

下载的内容
光盘内容
及公钥
网络接口
31
39
检测模块
36
缓冲区
34
RAM
验证模块
37
ROM
光盘
驱动器
33
35
40
CPU
输出装置
38
控制系统
32
输出信息

图3

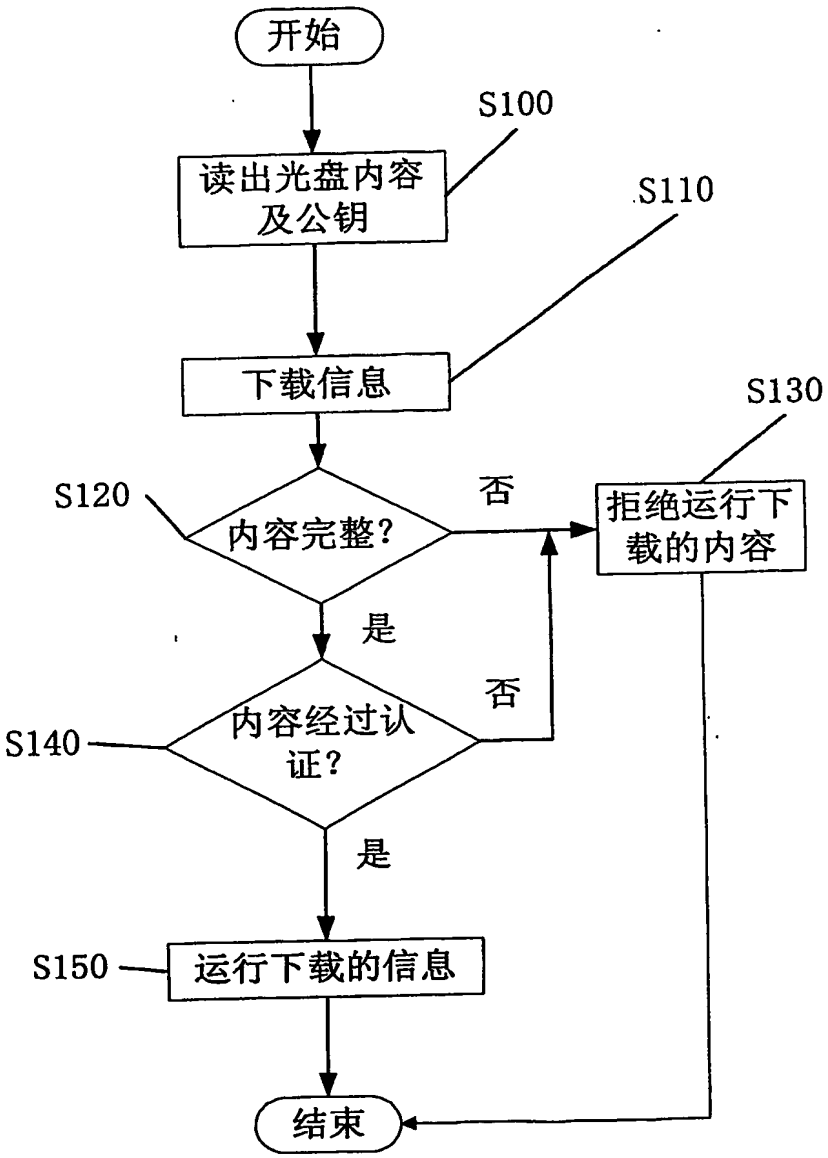

开始
S100
读出光盘内容及公钥
S110
下载信息
S130
S120
内容完整?
否
拒绝运行下载的内容
是
否
S140
内容经过认证?
是
S150
运行下载的信息
结束

图4